NOT MEASUREMENT
SENSITIVE

National Aeronautics and
Space Administration

NASA-STD-2804N
Effective September 7, 2010

MINIMUM INTEROPERABILITY SOFTWARE SUITE

NASA TECHNICAL STANDARD

FOREWORD

This standard is approved for use by NASA Headquarters and all NASA Centers and is intended to provide a common framework for consistent practices across NASA programs.

The material covered in this standard is governed and approved by the NASA Information Technology Management Board. Its purpose is to define the baseline software suite necessary to support interoperability both between NASA end user computers and within the NASA operating environment. The standard establishes Client Reference Configurations, Operating System Standards, and Compliance Dates for computers running Microsoft Windows, Apple Mac OS, and various Linux and UNIX operating systems. Adherence to this standard ensures compliance with federal requirements for desktop computers, laptops, and other end user devices.

Requests for information, corrections, or additions to this standard should be directed to the John H. Glenn Research Center at Lewis Field (GRC), Emerging Technology and Desktop Standards Group, MS 142-2, Cleveland, OH, 44135 or to *desktop-standards@lists.nasa.gov*. Requests for general information concerning standards should be sent to NASA Technical Standards Program Office, ED41, MSFC, AL, 35812 (telephone 256-544-2448). This and other NASA standard may be viewed and downloaded, free of charge, from the NASA Emerging Technology and Desktop Standards web page: http://etads.nasa.gov/current/2804.pdf .

/signature on file/

Linda Cureton
Chief Information Officer

This Page Left Blank Intentionally

Table of Contents

1 SCOPE

1.1 Purpose

This standard defines the baseline software suite necessary to support interoperability both between NASA end user computers and within the NASA operating environment. The standard establishes Client Reference Configurations, Operating System Standards, and Compliance Dates for computers running Microsoft Windows, Apple Mac OS, and various Linux and UNIX operating systems. Adherence to this standard ensures compliance with federal requirements for desktop computers, laptops, and other end user devices.

1.2 Applicability

Center CIO's will ensure that all NASA employees at their respective centers have access to an interoperable workstation that is equipped with a minimum software suite that meets the standards listed in Section 3 below.

The Client Reference Configuration (CRC) establishes required functionality and required products necessary to meet that functionality. Future procurements intended to address this functionality are restricted to the products defined in the CRC. Existing licenses for other products may not be renewed. Products will be added, replaced, or removed as appropriate to address agency interoperability requirements.

1.3 Waivers

The waiver process set forth in NPR 2800.1, paragraph 2.2.4, applies to this standard. The Emerging Technology and Desktop Standards group, in cooperation with the Office of the Chief Information Officer, will evaluate and process waivers as appropriate.

2 ACRONYMS AND DEFINITIONS

2.1 Acronyms

ASCS	Agency Security Configuration Standards
ASUS	Agency Security Update Service
CA	Certificate Authority
CIO	Chief Information Officer
CIS	Center for Internet Security
CRC	Client Reference Configuration
DAR	Data at Rest (encryption)
DSI	Desktop Smartcard Integration
ETADS	Emerging Technology and Desktop Standards
FDCC	Federal Desktop Core Configurations
FISMA	Federal Information Security Management Act
HTML	HyperText Markup Language
ICA	Independent Computing Architecture
IE	Internet Explorer
ISO	International Standards Organization
ITAR	International Traffic in Arms Regulations
IMAP	Internet Message Access Protocol
MIME	Multipurpose Internet Mail Extension
NCTR	NASA Client Trust Reference

NEF	NASA Electronic Forms
NIST	National Institute of Standards and Technology
NOCA	NASA Operational Certificate Authority
NOMAD	NASA Operational Messaging and Directory Service
OASIS	Organization for the Advancement of Structured Information Standards
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PDF	Portable Document Format
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
SBU	Sensitive But Unclassified
SCAP	Security Content Automation Protocol
SFTP	Secure File Transfer Protocol
SMTP	Simple Mail Transport Protocol
SSH	Secure Shell Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USGCB	United States Government Configuration Baseline
VPAT	Voluntary Product Accessibility Templates

2.2 Definitions

2.2.1 Basic Interoperability

Interoperability is the ability to obtain consistent and deterministic results within a specific platform (operating System Software, minimum hardware, required and optional software) as well as between platforms (PC, Mac, Linux) based on the established standards.

2.2.2 Desktop Computer

The term desktop computer is used generically to refer to traditional desktop systems as well as laptop computers, notebooks, tablets, engineering workstations, and similar platforms that are utilized to provide basic interoperability.

2.2.3 Support for Basic Interoperability

Systems supporting basic interoperability are defined as desktop computers used to exchange information electronically by end users that require any of the functionality listed in the Client Reference Configuration (Office Automation, Electronic Messaging, Web Browsing, etc. See section 3.3 Client Reference Configurations).

3 DETAILED REQUIREMENTS

3.1 Architectural Compliance Requirements

NASA has baselined and approved the NASA Integrated Information Technology Architecture[1]. The architecture is predicated on:

- The selection of standards for a broad and cost-effective infrastructure using commercial off-the-shelf and well-supported open source products to the greatest extent practical
- Interoperability both within and external to NASA

[1] NASA-STD-2814A, *NASA Integrated Information Technology Architecture—Technical Framework*

- Flexibility for future growth
- Consistency with generally accepted consensus standards as much as feasible
- Among these objectives, ensuring interoperability is one of NASA's most critical issues related to information technology.

In many cases, it is in NASA's best interest to specify commercial products as standards for an interoperable implementation of a particular set of related and integrated functions. The products themselves often include additional functionality or proprietary extensions not specified by this standard. While these products can be used to create higher-level interoperability solutions, these solutions may not be recognized within the context of the NASA interoperability environment and may be deprecated without warning by future revisions to this standard. Users of this standard are advised to apply appropriate caution when implementing proprietary or non-standard extensions, features and functions that go beyond the explicitly stated standard functionality.

3.2 Agency Security Configuration Standards

The NASA Office of the Chief Information Officer (OCIO) establishes Agency FISMA compliance goals and reporting requirements for NASA systems, through the use of Agency Security Configuration Settings, and the Agency Security Configuration Standards (ASCS) Project.

Compliance with the Agency Security Configuration Standards OCIO policy requires deployment of the NASA System Baselines to all systems. The NASA System Baselines for developed from the Federal Desktop Core Configurations (FDCC) settings for systems which have FDCC settings available, and requires the deployment of Center for Internet Security (CIS) Benchmarks, as reviewed by the ASCS Project, for all other systems.

To ensure compliance with federal and agency security requirements, including annual FISMA compliance goals and reporting requirements, security configuration settings are established and maintained by the Agency Security Configuration Standards (ASCS) Project.

The NASA Operating System Baseline Security Configurations are required by policy to be deployed to all interoperable systems. Application of the NASA Baseline configuration ensures compliance with NASA's approach to meeting the FISMA and FDCC requirements of the federal government. NASA Baseline security configurations for each operating system listed in this standard can be obtained at:

http://etads.nasa.gov/ASCS/

The United States Government Configuration Baseline (USGCB) will eventually replace FDCC for Windows 7 and Internet Explorer 8. See the ASCS website for details.

3.3 Client Reference Configurations

To address application, data, and infrastructure interoperability, and ensure compliance with federally mandated desktop computer configuration settings, the software functionality, applications, interface standards, configuration settings, versions, and deployment settings established by this standard are definitive.

Client Reference Configurations (CRC) are included for each operating system, with specific version and required configurations listed as appropriate. Interface standards are included to guide service providers and system integrators.

The Client Reference Configurations define the baseline upon which desktop service providers can define common enterprise images for all interoperable desktops computers. All IT initiatives funded or endorsed by the NASA OCIO account for systems that conform to the Client Reference Configurations. Application service providers and software developers can use the reference configurations to assist with integration and acceptance testing.

The NASA Emerging Technology and Desktop Standards group is working to ensure interoperability at the highest possible revision of products included in the Client Reference Configurations. Applications that meet these interface standards while providing improved end user experience, mitigating security risks, reducing support costs, or offering other tangible improvements may be submitted to desktop-standards@lists.nasa.gov for consideration in future revisions to these standards.

3.3.1 Client Reference Configuration for Windows XP

Client Reference Configuration for Windows XP					
Functionality	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Effective Date**
Operating System	Windows XP Professional		NASA FDCC Baseline Configuration settings[2]	Service Pack 3 with all security patches	September 30, 2008
	Windows XP Professional X64 Edition		NASA FDCC Baseline Configuration settings[3] KB968730 Hotfix[4]	Service Pack 2 with all security patches	April 1, 2009
Firewall	Windows Firewall		NASA FDCC Baseline Configuration settings[5]	XP/SP3	September 30, 2008
Smartcard Middleware	ActivIdentity ActivClient	NIST SP 800-73 Part 3	See section 3.4.6	XP 32-bit is 6.2.x XP x64 is 6.1.x	September 7, 2010
Data at Rest , Full Disk Encryption	McAfee Endpoint Encryption		Configured to use central policy and key escrow service See section 3.4.5	5.2.x	April 1, 2009
Content Encryption	Entrust ESP	Entrust Proprietary	See pki.nasa.gov	9.1.x	September 7, 2010
Secure Email	Entrust ESP	Entrust Proprietary	See pki.nasa.gov	9.1.x	September 7, 2010
Trust Anchor Management	NASA Client Trust Reference	X.509	See Section 3.7	2.x	June 24, 2008
Anti-Virus	Symantec Endpoint Protection		Enterprise update server	11.0.x	September 7, 2010
Anti-Malware	Symantec Endpoint Protection		Enterprise update server	11.0.x	June 24, 2008
Patch Reporting	PatchLink	Lumension Proprietary	Configured according to local Patchlink server requirements	6.4.x	June 30, 2008
	KBOX	KACE Proprietary		5.0.x	September 7, 2010
Web Browser	Mozilla Firefox	W3C and industry standards, including the following: HTML 4.01 XHTML 1.0 CSS 2 (Cascading Style Sheets) ECMAscript (JavaScript) capability to run Java 2 applets, SSL version 3, TLS 1.0	See sections 3.4.6 and 3.7	3.6x	September 7, 2010
	Microsoft Internet Explorer		NASA FDCC Baseline Configuration settings. Also see sections 3.4.6 and 3.7	8.0.x	September 7, 2010
Office Automation	Microsoft Office (Professional Edition with Outlook)			2007 SP2	April 1, 2009
Word Processing	Microsoft Word	Office Open XML document format	Configure to use Office Open XML file format by default	2007 SP2	April 1, 2009

[2] Check http://etads.nasa.gov/ASCS/ for current configurations
[3] Check http://etads.nasa.gov/ASCS/ for current configurations
[4] Supplemental hotfix to support SHA-2 encryption algorithms
[5] Check http://etads.nasa.gov/ASCS/ for current configurations

Client Reference Configuration for Windows XP

Functionality	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Effective Date**
Spreadsheet	Microsoft Excel	Office Open XML document format	Configure to use Office Open XML file format by default	2007 SP2	April 1, 2009
Presentation	Microsoft PowerPoint	Office Open XML document format	Configured to use Office Open XML file formats by default	2007 SP2	April 1, 2009
Electronic Mail	Microsoft Outlook	NASA-STD-28015, IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	2007 SP2	April 1, 2009
Calendaring	Microsoft Outlook as implemented by NOMAD	iCalendar (RFC 2445)[6]		2007 SP2	April 1, 2009
Instant Messaging	Communicator	SIP	Enterprise LCS Settings as implemented by NOMAD Pidgin-sipe LCS/OCS plugin	2005	June 24, 2008
	Pidgin	XMPP	NASA Jabber Service Pidgin-sipe LCS/OCS plugin	2.6.x	June , 2009
PDF Viewer	Adobe Reader	PDF		9.3.x	September 7, 2010
Java	Java run-time environment		With all security patches	Java 6	October 1, 2008
Audio/video players (all are required	Apple QuickTime Player	Various Multimedia	Default for QuickTime formats	7.6.x	June 24, 2008
	Adobe Flash Player	Flash SWF		10.1.x	September 7, 2010
	Microsoft Windows Media Player	Windows Media Files	Default for all supported formats	12.0.x	June 24, 2008
	Silverlight	Various Multimedia		4.0.x	September 7, 2010
	Apple iTunes	Various Multimedia		9.2.x	September 7, 2010
Access to centrally served Windows applications	Citrix ICA Client	Citrix ICA ProtocolXenApp Plugin		11.2.x	June 24, 2009
Electronic Forms	FileNet Desktop e-Forms	See Section 3.6	NASA Distribution Center	4.2	June 24, 2008
Video Conferencing	Secure Virtual Team Meeting		https://nasa.webex.com		August 2010

[6] This standard provides limited interoperability

3.3.2 Client Reference Configuration for Windows 7

Client Reference Configuration for Windows 7					
Functionality	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Effective Date**
Operating System	Windows 7 Enterprise or Ultimate		NASA Baseline Security settings[7]		September 7, 2010
	Windows 7 Enterprise or Ultimate X64 Edition		NASA Baseline Security settings[8]		September 7, 2010
Firewall	Windows Firewall		NASA Baseline Security settings[9]		September 7, 2010
Smartcard Middleware	ActivIdentity ActivClient	NIST SP 800-73 Part 3	See section 3.4.6	6.2.x	September 7, 2010
Data at Rest, Full Disk Encryption	McAfee Endpoint Encryption		Configured to use central policy and key escrow service See section 3.4.5	5.2.x	September 7, 2010
Content Encryption	Entrust	Entrust Proprietary	See pki.nasa.gov	9.1.x	September 7, 2010
Secure Email	Entrust Desktop Solution	Entrust Proprietary	See pki.nasa.gov	9.1x	September 7, 2010
Trust Anchor Management	NASA Client Trust Reference	X.509	See Section 3.7	2.x	September 7, 2010
Anti-Virus	Symantec Endpoint Protection		Enterprise update server	11.0.X	September 7, 2010
Anti-Malware	Symantec Endpoint Protection		Enterprise update server	11.0.X	September 7, 2010
Patch Reporting	PatchLink	Lumension Proprietary	Configured according to local Patchlink server requirements	6.4.x	September 7, 2010
	KBOX	KACE Proprietary		5.0.x	September 7, 2010
Web Browser	Mozilla Firefox	W3C and industry standards, including the following: HTML 4.01 XHTML 1.0 CSS 2 (Cascading Style Sheets) ECMAscript (JavaScript) capability to run Java 2 applets, SSL version 3, TLS 1.0	See sections 3.4.6 and 3.7	3.6.x	September 7, 2010
	Microsoft Internet Explorer		NASA FDCC Baseline Configuration settings. Also see sections 3.4.6 and 3.7	8.0.x	September 7, 2010
Office Automation	Microsoft Office (Professional Edition with Outlook)			2007 SP2	September 7, 2010
Word Processing	Microsoft Word	Office Open XML document format	Configure to use Office Open XML file format by default	2007 SP2	September 7, 2010
Spreadsheet	Microsoft Excel	Office Open XML document format	Configure to use Office Open XML file format by default	2007 SP2	September 7, 2010

[7] Check http://etads.nasa.gov/ASCS/ for current configurations
[8] Check http://etads.nasa.gov/ASCS/ for current configurations
[9] Check http://etads.nasa.gov/ASCS/ for current configurations

Client Reference Configuration for Windows 7

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
Presentation	Microsoft PowerPoint	Office Open XML document format	Configure to use Office Open XML file formats by default	2007 SP2	September 7, 2010
Electronic Mail	Microsoft Outlook	NASA-STD-28015, IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	2007 SP2	September 7, 2010
Calendaring	Microsoft Outlook as implemented by NOMAD	iCalendar (RFC 2445)[10]		2007 SP2	September 7, 2010
Instant Messaging	Communicator	SIP	Enterprise LCS Settings as implemented by NOMAD Pidgin-sipe LCS/OCS plugin	2005	September 7, 2010
	Pidgin	XMPP	NASA Jabber Service Pidgin-sipe LCS/OCS plugin	2.6.x	September 7, 2010
PDF Viewer	Adobe Reader	PDF		9.3x	September 7, 2010
Java	Java run-time environment		With all security patches	Java 6	September 7, 2010
Audio/video players (all are required)	Apple QuickTime Player	Various Multimedia	Default for Quicktime formats	7.6.x	September 7, 2010
	Adobe Flash Player	Flash SWF		10.1.x	September 7, 2010
	Microsoft Windows Media Player	Windows Media Files	Default for all supported formats	12.0.x	September 7, 2010
	Silverlight	Various Multimedia		4.0.x	September 7, 2010
	Apple iTunes	Various Multimedia		9.2.x	September 7, 2010
Access to centrally served Windows applications	Citrix ICA Plugin	Citrix ICA ProtocolXenApp Plugin		11.2.x	September 7, 2010
Electronic Forms	FileNet Desktop e-Forms	See Section 3.6	NASA Distribution Center	4.2	September 7, 2010
Video Conferencing	Secure Virtual Team Meeting		https://nasa.webex.com		September 7, 2010

[10] This standard provides limited interoperability

3.3.3 Client Reference Configuration for Mac OS X

Client Reference Configuration for Mac OS X					
Functionality	**Application**	**Interface Standards**	**Required Settings**	**Version**	**Effective Date**
Operating System	Mac OS X		CIS Benchmarks	10.6.x	April 1, 2010
Firewall	Apple Firewall		Allow essential services Enable firewall logging Enable Stealth Mode[11]		April 1, 2009
Smartcard Middleware	Bundled with OS		See Section 3.4.6		April 1, 2010
PKI	Entrust Secure Desktop for Mac (SDM)		NASA PKI Team specified settings	8.0	July 2, 2010
Trusted CA Certificates	See Section 3.7	X.509		3	June 24, 2008
Anti-Virus	Symantec Antivirus Enterprise			10.2.x	December 2008
Anti-Malware	Symantec Antivirus Enterprise			10.2.x	December 2008
Data at Rest Encryption			Configured to use central policy and key escrow service See section 3.4.5	Not Available	Not Available
Home Folder Encryption	FileVault	Apple Proprietary		Bundled	September 7, 2010
Web Browser	Mozilla Firefox	W3C and industry standards, including the following: HTML 4.01 XHTML 1.0 CSS 2 (Cascading Style Sheets) ECMAscript (JavaScript) capability to run Java 2 applets, SSL version 3, TLS 1.0	See sections 3.4.6 and 3.7	3.6.x	July 1, 2010
	Apple Safari		See sections 3.4.6 and 3.7	5.0.x	July 2009
Java	Java Run-time Environment		With all security patches	Java 6	October 1, 2008
Office Automation	Microsoft Office 2008 for Mac			2008	April 1, 2009
Word Processing	Microsoft Word 2008 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	12.2.x	April 1, 2009
Spreadsheet	Microsoft Excel 2008 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	12.2.x	April 1, 2009
Presentation	Microsoft PowerPoint 2008 for Mac	Office Open XML document format	Configure to use Office Open XML file formats by default	12.2.x	April 1, 2009

[11] Vendor terminology for these settings

Client Reference Configuration for Mac OS X					
Functionality	**Application**	**Interface Standards**	**Required Settings**	**Version**	**Effective Date**
Electronic Mail	Microsoft Entourage 2008 for Mac Web Services Edition	NASA-STD-28015, IMAP4, SMTP, IMAP over SSL/TLS	Configured for access to NOMAD	13.0.x	July 1, 2010
	Apple Mail		Integration with NOMAD limited to email only	4.2.x	April 1, 2010
Calendaring	Microsoft Entourage 2008 for Mac Web Services Edition as implemented by NOMAD	iCalendar (RFC 2445)[12]	Configured for access to NOMAD	13.0.x	April 1, 2009
	Apple iCal	iCalendar (RFC 2445)[13]	Configured for access to NOMAD	4.0.x	July 2010
Instant Messaging	Microsoft Messenger	SIP	Enterprise LCS Settings as specified by NOMAD	6.0.x	June 24, 2008
	Apple iChat	XMPP	NASA Jabber Service settings	Bundled	June 24, 2008
Patch Reporting	PatchLink (Update)	Lumension proprietary	Configuration for Server info	6.4.x	June 30, 2008
	KBOX	Kace Proprietary		5.0.x	September 7, 2010
Audio/video players (all are required)	Apple QuickTime Player	Various Multimedia		7.6.x	June 24, 2008
	Adobe Flash Player	Flash SWF		10.1.x	June 24, 2008
	Telestream Flip4Mac WMV	Windows Media	Default for Windows Media	2.3.x	June 24, 2008
	SilverLight	Various Multimedia		4.0.x	July 1, 2010
	Apple iTunes	Various Multimedia	Default for all supported formats	9.2.x	July, 1, 2010
PDF Viewer	Apple Preview			5.0.x	April 1, 2010
Access to centrally served Windows applications	Citrix ICA Client	Citrix ICA Protocol XenApp Plugin		11.1.x	
Electronic Forms	FileNet Desktop e-Forms	See Section 3.6	NASA Distribution Center	4.2	June 24, 2008
Video Conferencing	Secure Virtual Team Meeting		https://nasa.webex.com		August 2010

[12] This standard provides limited interoperability

[13] This standard provides limited interoperability

3.3.4 Client Reference Configuration for Linux

Client Reference Configuration for Linux*					
Functionality	**Application**	**Interface Standards**	**Required Settings**	**Version**	**Effective Date**
Operating System	Red Hat Enterprise Linux Desktop with Workstation option		CIS Benchmarks	5.3 or later	June 24, 2008
	Ubuntu		CIS Benchmarks	10.0.4	July 2010
Firewall	Bundled		Control inbound and outbound connections enabled by default	Bundled	June 24, 2008
Smartcard Middleware	ActivIdentity ActivClient		See Section 3.4.6	32-bit 3.0.x 64-bit Unsupported	September 2010
Secure Email	Thunderbird	S/MIME	Use exported NOCA certificates See pki.nasa.gov	3.0.x	September 7, 2010
Trusted CA Certificates	See Section 3.7	X.509		3	June 24, 2008
Anti-Virus	Symantec Antivirus for Linux			1.0.x	July 2010
Data at Rest Encryption	McAfee Endpoint Encryption		Configured to use central policy and key escrow service	Not Available	Not Available
Patch Reporting	PatchLink (Update)	Lumension Proprietary	Configuration for Server info	6.4.x	June 30, 2008
	KBOX	Kace Proprietary		5.0.x	September 7, 2010
Web Browser	Mozilla Firefox	W3C and industry standards, including the following: HTML 4.01 XHTML 1.0 CSS 2 (Cascading Style Sheets) ECMAscript (JavaScript) capability to run Java 2 applets, SSL version 3, TLS 1.0		3.6.x	July 2010
Office Automation	OpenOffice.org	OASIS Open Document Format for Office Applications (OpenDocument		3.1.x	June 2009
Word Processing	OpenOffice Writer	OASIS Open Document Format for Office Applications (OpenDocument	Configure to use Office Open XML file format by default	3.1.x	June, 2009
Spreadsheet	OpenOffice Calc	OASIS Open Document Format for Office Applications (OpenDocument	Configure to use Office Open XML file format by default	3.1.x	June, 2009
Presentation	OpenOffice Impress	OASIS Open Document Format for Office Applications (OpenDocument	Configure to use Office Open XML file format by default	3.1.x	June, 2009
Electronic Mail	Mozilla Thunderbird	NASA-STD-28015, IMAP4, SMTP, IMAP over SSL/TLS	Configured for access to NOMAD	3.0.x	June 24, 2008

Client Reference Configuration for Linux*					
Functionality	**Application**	**Interface Standards**	**Required Settings**	**Version**	**Effective Date**
Calendaring	NOMAD Outlook Web Access	iCalendar (RFC 2445)[14], HTTPS	Web Browser	2.x	June 24, 2008
Instant Messaging	Not Available	SIP	Enterprise LCS Settings as specified by NOMAD Pidgin-sipe LCS/OCS plugin		
	Pidgin	XMPP	NASA Jabber Service settings	2.4.x	June 24, 2008
Java	Java run-time environment		With all security patches	Java 6	June 24, 2008
Audio/video player	MPlayer	Multimedia	Default for supported formats	1.0	June 24, 2008
	Adobe Flash Player			10.1.x	June 24, 2008
PDF Viewer	Adobe Reader			9.3.x	September 7, 2010
Access to centrally served Windows applications	Citrix ICA Client	Citrix ICA		11. 10.0.x	June 24, 2008
Electronic Forms	FileNet Desktop E-Forms		Citrix ICA		
Video Conferencing	Secure Virtual Team Meeting		https://nasa.webex.com		August 2010

* When the vendor provides bundled support for applications included in the CRC, the vendor-provided and supported versions should supersede those of the CRC.

[14] This standard provides limited interoperability

3.4 Additional Client Reference Configuration Guidance

3.4.1 Office Automation Applications

The default document format for Microsoft Office 2007(SP2), Microsoft Office 2008 for Mac, and OpenOffice on Linux systems is the ISO Standard Office Open XML format.

Microsoft Office 2007 (SP2) Standard Edition (or better) is required on all interoperable Microsoft Windows systems. As of April 2009, all interoperable Microsoft Windows systems were required to run Office 2007.

Microsoft Office 2008 for Mac (Standard Edition) is required on all interoperable Mac OS X systems. As of April 2009, all interoperable Mac OS X systems were required to run Office 2008. Note: Office 2008 discontinues support Visual Basic for Applications.

Microsoft Office 2010 (Office 14.0)[15] was released on June 15, 2010, and is approved for deployment in December 2010.

Microsoft Office 2011 for Mac is expected to be released in October 2010 and will feature a Mac version of Outlook to replace Entourage. Additional guidance on the deployment of Office 2011 for Mac will be made available as appropriate. Note: Office 2011 reinstates support for Visual Basic Applications.

OpenOffice is approved for deployment and use on all Linux platforms and supports the standard Office Open XML file format. Documents created with Microsoft Office do not always render perfectly in OpenOffice, and vice versa.

3.4.2 Electronic Messaging

NASA has implemented an enterprise-wide electronic messaging service known as NOMAD. This service provides integrated email, calendaring, scheduling, contact management, and instant messaging. All interoperable desktops are required to be configured to access this environment.

Note that while NOMAD is based upon open standards and can support stand-alone email clients that adhere to the defined interface standards of the Client Reference Configurations, utilizing such clients limit end user interoperability, may not be supported by NOMAD, and may result in future inability to participate in the enterprise messaging environment.

Supported Messaging Clients

Windows:	Microsoft Outlook
Mac OS X:	Microsoft Entourage and Apple Mail
Linux:	Mozilla Thunderbird

Apple Mail now supports the NOMAD calendar and scheduling environment but does have some integration issues. The choice of client on Mac OS X depends upon the required functionality. In some cases, Microsoft Entourage is more appropriate (for instance, when delegation functionality is required). In other cases Apple Mail and iCal with Address Book is suitable.

[15] Note that Office 2010 has been given the version number 14.0, despite the fact that its immediate predecessor, Office 2007, was designated by the version number 12.

Additional clients which conform to the interface standards may be used as point solutions where interoperability might otherwise not be available.

The selection of mail clients will continue to promote secure access to commercial and partner email services in support of extra-Agency (non-NOMAD) collaborative activities.

3.4.3 Web browser

Internet Explorer 7 (IE7) can continue to be used on Windows XP. IE7 must be removed from all systems by October 2013.

Internet Explorer 8 (IE8) is approved for deployment on NASA desktops. IE8 is a NASA standard browser and shall be installed on all interoperable Windows systems. The NASA System Configuration Baseline must be used for IE8.

Internet Explorer 9 (IE9) is in beta, and is currently undergoing evaluation and interoperability testing. When Internet Explorer 9 becomes commercially available, and has been thoroughly tested for use in NASA a deployment timeline will be established.

Firefox 3.6.x is the standard for Windows, Macintosh and Linux systems. Firefox 3.5.x must be removed from all systems by August 2010 after which time Mozilla will cease to support Firefox 3.5

Safari 5.0.x is the standard for all interoperable Macintosh systems. Safari 5.0.x is approved for immediate deployment. Apple released Safari 5.0.x to address security vulnerabilities present in Safari 4.0.x. The use of Safari on Windows is not supported.

Browsers should be configured with the agency approved list of Trust Anchors as found in the NASA Client Trust Reference (NCTR). Some browsers will require additional setting, also found at the NCTR site.

http://etads.nasa.gov/DCS/ClientTrustReference.shtml

3.4.4 PatchLink

The Agency is transitioning to KACE KBOX for patch reporting and patch management. The current product, Patchlink, will be used until new patch reporting solution is implemented.
For current information on the Patchlink Agent, including specific version levels, please refer to the Agency Security Update Service (ASUS) web site at https://patches.ksc.nasa.gov/

Patchlink 6.4 contains a SCAP-validated FDCC reporting module and must be installed on all systems.

3.4.5 Data at Rest (DAR) Encryption

NASA has purchased a suite of software from McAfee (previously Safeboot) to provide encryption for data at rest. This software is compliant with federally mandated requirements for encryption of sensitive data on mobile devices (including laptops and removable media). Licenses will be made available to all NASA employees and onsite contractors. All laptops, all desktops with Personally Identifiable Information (PII) or other similarly sensitive data[16], and all new and refreshed computers are required to implement this encryption technology. The first

[16] e.g. ITAR, SBU

phase of the implementation focuses on laptops and system containing PII data. Please contact your local DAR representative for Center specific deployment details
McAfee's solution for the Macintosh platform is currently in Beta. After the product is released it will be evaluated for interoperability and a deployment timeline developed. For more information see http://etads.nasa.gov/DAR/

3.4.6 Desktop Smartcard Integration Configuration Requirements

The Desktop Smartcard Integration Team develops software and configuration requirements for smartcard use and authentication on as the NASA standard operating systems. See the NASA Desktop Smartcard Integration Configuration Requirements page at http://etads.nasa.gov/DSI/CR for additional information for middleware, smartcard desktop authentication and browser authentication configuration settings.

3.5 Operating System Standards, Timelines, and Compliance Dates

3.5.1 Microsoft Windows XP

All Windows XP systems must be compliant with the NASA FDCC Baseline configuration.

Windows XP must be removed from all NASA systems by October 2013.

3.5.1.1 Microsoft Windows XP 64-bit

Windows XP Professional x 64 Edition is specified as the standard version of Windows 64 bit for the agency interoperable computing environment and is subject to the Windows XP Client Reference Configuration.

Windows XP Professional x 64 Edition should be removed from all NASA systems by October 2013.

3.5.2 Microsoft Windows Vista

Microsoft Windows Vista shall not be deployed. The earlier decision to deploy Microsoft Windows Vista has been rescinded. All Vista systems must be compliant with the NASA FDCC Baseline configuration settings.

Vista must be removed from all NASA systems by October 2013.

3.5.3 Microsoft Windows 7

Microsoft Windows 7 – Enterprise and Ultimate editions only – are approved for deployment. The 64 bit version of Microsoft Windows 7 shall be deployed to all new and refreshed (upgraded) systems. 32 bit versions of Microsoft Windows 7 may be installed if necessary to support non-64 bit capable applications.

Existing Windows XP and Vista systems shall be upgraded to either the 64 bit version of Windows 7 or the 32 bit version depending on hardware capability and software dependency.

Windows 7 shall be required by October 2013.

3.5.4 Mac OS

Mac OS X 10.6 (Snow Leopard) is the currently supported operating system on all Intel based interoperable Macintosh systems. . At the time of this writing, Mac OS X 10.6.4 is the current maintenance release. Mac OS X 10.6 shall be installed on all Intel based Macs by June 1, 2011. Older versions should be removed from the environment. As always, the operating system must be kept up-to-date with vendor patches

Mac OS X 10.6 shall be required on all Intel based Macs June 1, 2011.

Mac OS X 10.6 provides smartcard authentication services as part of the operating system. As Mac OS X 10.6 does not run on non-Intel based Macs, these systems will be considered non-interoperable when smartcard use is required.

3.5.5 Linux/x86 and x86-64

UNIX and Linux systems with no need for interoperability need not comply with the interoperability requirements in this standard. Such systems would include special-purpose computers such as name servers, compute servers, data acquisition systems, special software development workstations, or other components of the overall computing infrastructure.

Several product standards are not available for any Linux or UNIX system. In order to comply with this standard, interoperable desktops must have some way to access these products. It is recommended to use the Citrix ICA client to connect to a Microsoft Windows application server.

Two Linux distributions are supported for use on interoperable desktops:
Red Hat Enterprise Linux Desktop 5 with Workstation option:

https://www.redhat.com/rhel/desktop/

Ubuntu 10.0.4

http://www.ubuntu.com/

All new and refreshed Linux systems must run one of the two supported Linux distributions. SuSE Linux Enterprise Desktop has been removed from the standard. SuSE Linux users should be migrated to one of the two supported Linux distros at their earliest convenience. SuSE Linux should be removed from the environment by January 2012.

3.5.6 Other UNIX

The following UNIX systems are supported in the NASA interoperable computing environment. Generally, both the current version and prior version of the operating system are acceptable. However, the older version of the operating system must continue to be supported by the vendor, and like all systems, must be kept current with security patches.

3.5.6.1 Sun Solaris/SPARC, x86, and x86-64

Solaris is at version 10. Information about supported Solaris releases may be found at:

http://www.sun.com/software/solaris/faqs/general.jsp#releases

3.5.6.2 IBM AIX/POWER

AIX 5L 5.2 and 5.3 are current. AIX versions are described at:

http://www-1.ibm.com/servers/aix/os/index.html

3.5.6.3 HP HP-UX/PA-RISC

HP-UX 11i v3 is current. The HP-UX 11i web page is at:

http://www.hp.com/products1/unix/operating/index.html

3.6 Electronic forms

Agency requirements for a forms product include the ability to provide access to all NASA employees requiring access to forms (including filler operation across all NASA standard desktop platforms), the capability to enhance NASA business processes through intelligent functionality, ease of use, and an array of functional and operational capabilities.

Since an open application program interface standard for data interchange among forms products has not yet been adopted or approved by any acknowledged standards body, a product-level selection was warranted. After an evaluation of commercial products, FileNet Desktop eForms was found to comply with all key requirements. Other products which meet the requirements and interoperate with the FileNet product may be used via the waiver process.

Agency-level forms used for data collection with an official assigned number must be FileNet forms. Center unique versions of these agency forms should not be created or used.

NASA has purchased an Agency agreement for the use of FileNet Desktop eForms to allow all NASA centers, recognized partners, qualified contractors/service providers, and the general public the use of the product to complete forms when doing business with NASA. This includes center-specific forms, as well as other forms needed in the process of doing business.

Agency forms and software downloads are available through the NASA Electronic Forms (NEF) website http://nef.nasa.gov. The NEF website is the central repository for all forms used within NASA (NASA Forms, Standard Forms, Optional Forms, Center-specific forms, etc.), and is available to all internal users and external partners. For the purpose of form distribution an Agency distribution center profile has been created to allow access to Agency forms. All forms users should have the NEF distribution center profile, in addition to all of the profiles established for access to center-specific, and contractor maintained form collections. These profiles are maintained and distributed through the NEF website.

3.7 Public Key Infrastructure Relying Party Requirements

3.7.1 Additional X.509 Root Certificates

There are normally multiple local trusted Certificate Authority (CA) certificate stores in addition to those supplied by the operating system vendor: including, but not limited to, Java, Mozilla Thunderbird, and Mozilla Firefox.

On Windows and Mac OS (and on other systems where it is feasible to do so), the following X.509 root certificates must be installed as trusted roots in the local certificate stores:

- NASA Data Center Certificate Authority
- NASA Operational Certificate Authority (NOCA) from http://pki.nasa.gov
- Federal Bridge Certificate Authority
- U.S. Treasury roots from http://pki.nasa.gov
- Federal PKI Common Policy

3.7.2 Additional Relying Party Requirements

All client applications that perform PKI operations shall be required to support the SHA-2 family hashing algorithms, by November 2010. Information on SHA-2, RSA, and encryption algorithm lifetimes and accompanying NIST documentation (SP800-78-2, SP800-131) is available at http://pki.nasa.gov.

3.7.3 NASA Client Trust Reference

The NASA Client Trust Reference (NCTR) repository can be found on the ETADS web site at: http://etads.nasa.gov/DCS. Trusted Sites and Certificates are listed in the NASA Client Trust Reference (NCTR) when they are presumed to be required on the majority of NASA end user systems, or required to enable Agency level business functions for groups of personnel appreciably larger than those at any single NASA Cen*ter.*

3.8 Section 508 Compliance Requirements

Software products procured after June 21, 2001 must be in conformance with Section 508 of the Rehabilitation Act. Complete information and guidance on addressing Section 508 requirements is available at:

http://www.section508.nasa.gov

When developing and testing software, users are reminded to use the recommended tools for evaluation:

Function	Windows	Mac OS X	Linux
Screen Reading Software	JAWS 8.x or higher	VoiceOver	
	Window Eyes 6.x or higher		
Desktop Automated Tool	HiSoftware ACCVerify Deque Ramp	Deque Ramp	
PDF Documents	Adobe Acrobat 8.x or higher	Adobe Acrobat 8.x or higher	
	NetCentric Technologies CommonLook Plug-in for Acrobat		

The NASA Emerging Technologies and Desktop Standards team has evaluated vendor-supplied Voluntary Product Accessibility Templates (VPAT) for Windows XP, Windows Vista, Windows 7, Mac OS X Snow Leopard, Office 2007, and Firefox 3.6.x, and believes that they satisfy the Section 508 requirements to an acceptable degree.

3.9 FIPS 140-2 Compliance Requirements

NASA will adhere to the guidelines and recommendations of the National Institute of Standards and Technology as required by the Federal Information Security Management Act, particularly as they apply to computer security and encryption technology for desktop hardware and software. More specifically, NASA will comply with Federal Information Processing Standards (FIPS) 140-1 and 140-2 as applicable, validated encryption modules become available.

NASA application developers and service providers are reminded that whenever cryptographic-based security systems are used to protect sensitive information in computer systems, the cryptographic modules utilized must be FIPS 140-2 compliant as validated by NIST[17]. A current list of validated products can be found at:

http://csrc.nist.gov/cryptval/

The following products mentioned in NASA-STD-2804 have been validated by a NIST-accredited testing laboratory and may be appropriate to protect sensitive information with cryptography under specific conditions:

Product	**Validation Module**	**Certification**	**Comments**
Microsoft Internet Explorer	Kernel Mode Cryptographic Module for Windows XP	#997	Single User Mode, FIPS 140-1
Microsoft Outlook	Outlook Cryptographic Provider	#110	Single User Mode, FIPS 140-1, S/MIME
Entrust PKI Software	Entrust Entelligence Kernel Mode Cryptographic module	#1043	Single User Mode, FIPS 140-2
F-Secure SSH	F-Secure® Cryptographic Library™ for Windows	#437	FIPS 140-2, When operated in FIPS Mode, Single User Mode.
F-Secure SSH	F-Secure® Cryptographic Library™ for Linux	#776	FIPS 140-2, When operated in FIPS Mode, Single User Mode.
OpenSSL	OpenSSL FIPS Object Module (1.2)	#1051	
Citrix ICA Client for Windows	Kernel Mode Cryptographic Module for Windows XP	Not Validated	Uses MS Windows FIPS Crypto Module
McAfee Endpoint Encryption for PCs Client	Diffie-Hellman	#1131	FIPS 140-2, When operated in FIPS Mode
Mozilla NSS	Network Security Services (NSS)	#1280	FIPS 140-2, When operated in FIPS Mode
Entrust PKI Software	L Version 8.0	#797 #1043	FIPS 140-2, When operated in FIPS Mode

3.10 Wireless Requirements

The current minimum wireless hardware and software configuration that will be used by NASA to support interoperability is defined in NASA-STD-2850.1. For information on the ongoing conditions that wireless infrastructure devices must satisfy to connect to the NASA network see NASA-STD-2850.1 which when posted will be available at http://standards.nasa.gov/.

3.11 Energy Management

In order to comply with Executive Order 13423, printers, laptops and desktop systems must be configured to use energy-saving settings.

3.11.1 Computers

Requirements:

[17] Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*

- Displays shall be set to sleep after 15 minutes of idle time
- Systems shall go to sleep after 60 minutes of idle time

Wake-on-LAN functionality may be useful for administrators to wake the systems in order to perform maintenance.

Generally, the level of sleep should be as effective as possible at saving power, given the constraints of the environment. The S3 power savings mode (keep memory contents intact, and listen for a wake signal) is suitable in most circumstances.

Servers and other special-purpose systems are exempted from this requirement.

3.11.2 Printers

Where possible, duplex printing should be utilized. Networked printer drivers should be configured to utilize duplex printing by default. Only duplex capable printers should be purchased.

3.12 Virtualization

Virtualization technology allows multiple operating systems to be run on a single physical computer. If a desktop virtualization product is required for interoperability the recommended solution (VMWare) must be used. See Table of Optional Software. The virus protection software listed in the Client Reference Configuration shall be used with Virtualization products.

4 ADDITIONAL SOFTWARE TABLES

4.1 Table of Optional Software

The following table contains optional useful functionality that is not required for interoperability. These software applications and utilities can be made available to end users upon request or distributed with standard enterprise images to support interoperability. Where practical, it is recommended that these tools be used rather than similar tools that address the same function. This table often identifies software that will eventually be included in the Client Reference Configurations.

Function	Windows	Mac OS X	Linux
3279 client	QWS3270	tn3270	tn3270
ssh client	XWin32	bundled	bundled or OpenSSH
sftp client	FileZilla	Cyberduck	bundled or OpenSSH
Advance file archive extractor/creator	WinZip 12	bundled	bundled
Real A/V Player	RealPlayer 11	RealPlayer 11	RealPlayer 11
Remote access to Windows systems	MS Remote Desktop Connection	MS Remote Desktop Connection	bundled
X window system server	Exceed	Apple X11	bundled
PostScript previewer	Ghostscript	bundled	bundled
PDF creator	Adobe Acrobat, Pro	Adobe Acrobat Pro	Scribus
PDF writer/converter	PrimoPDF, MS Office 2007 PDF plug-ins	bundled	bundled
Project Management	MS Project 2007	OpenProj	OpenProj

Virtualization	VMWare Workstation	VMWare Fusion	VMWare Workstation

4.2 Table of Agency Required Software

The following table summarizes software that must be installed on all Agency desktop systems, regardless of their interoperability requirements.

This software is included in the Client Reference Configuration.

Agency Required Software

Function	Windows	Mac OS X	Linux	Unix
FISMA compliance	FDCC/NASA System Configuration Baselines	CIS Benchmarks	CIS Benchmarks	CIS Benchmarks
Patch reporting	Patchlink/KACE KBOX	Patchlink/KACE KBOX	Patchlink/KACE KBOX	Patchlink/KACE KBOX
Anti-Virus	Symantec Endpoint Protection	Symantec Anti-Virus Enterprise Edition	Symantec	Symantec
Data-at-Rest Encryption	McAfee Endpoint Encyption	McAfee Endpoint Encyption[18]	McAfee Endpoint Encyption[19]	McAfee Endpoint Encyption[20]
FIPS 201 Authentication	ActivClient	Bundled with OS	ActivClient	ActivClient

5 REVIEW AND REPORTING REQUIREMENTS

5.1 Interoperability Maintenance Reporting

Upon request, Center CIO’s will provide the NASA CIO with a summary report, outlining the status of minimum interoperability access for each NASA employee.

5.2 Interoperability Reporting

Each Center CIO will utilize the Agency selected processes and tools, both manual and automated, to report on an annual basis to the NASA CIO the hardware and software configuration of all workstations at their respective Centers. This data will contain sufficient information to ascertain if the workstation supports NASA employees or is Government-furnished equipment to a contractor, whether the equipment is required to be interoperable, and a description of the hardware architecture/environment. The report will specify the number of NASA employees that do not have access to interoperable workstations.

5.3 Basic Interoperability Standards Maintenance

This standard, and its companion, NASA-STD-2805 Minimum Hardware Configurations, are maintained on behalf of the NASA CIO by the Emerging Technology and Desktop Standards group. Together, these standards define the software, hardware, and configurations necessary to ensure basic interoperability within the NASA information technology computing infrastructure.

[18] Pending vendor availability
[19] Pending vendor availability
[20] Pending vendor availability

This standard will be reviewed and updated on an as-required basis, not to exceed 12-month intervals. Participation in the revision process is open to all NASA employees. Details on how to be alerted of changes to the standards and/or comment on proposed updates can be found at:

http://desktop-standards.nasa.gov

This site also maintains interim guidance, position papers, software and hardware reviews, recommendations and other documentation intended to promote standardized basic interoperability.

6 DURATION

6.1 Duration

This standard will remain in effect until canceled or modified by the NASA CIO.

7 SUPPORTING DOCUMENTS

7.1 Supporting Documents

Supporting documents and additional information related to this standard may be found at:

http://desktop-standards.nasa.gov